Amendments to the Claims:

Re-write the claims as set forth below. This listing of claims will replace all prior versions and listings, of claims in the application:

Listing of the Claims:

1. (allowed) A method for a computing system to provide protection of incoming data, the method comprising the steps of:

receiving, by a video decoder of the computing system, data of at least one of analog audio data and analog video data, wherein a line of the data includes screen end information, a data access parameter, color burst information, and at least one of audio and video data and wherein the data access parameter is independent of a source of the data;

digitizing, by the video decoder independent of the data access parameter, the at least one of audio and video data to produce digital video, wherein, once the at least one of audio and video data is digitized, the data access parameter is lost;

prior to enabling a central processing unit to access the digital video, determining by a graphics controller whether the data access parameter restricts accessing of the digital video; and

when the data access parameter restricts accessing of the digital video, preventing the central processing unit from accessing the digital video without restriction.

2. (allowed) The method of 1 further comprises, within step (a), receiving the date from at least one of: a digital video disc driver within the computing system, a video cassette recorder, and a video transmission source.

3. (allowed) The method of claim 1, wherein the data access parameter comprises at least one of: copy restrictions and parental control.

4. (allowed) A video decoder system comprising:

a processing circuit; and

memory that stores programming instructions that, when read by the processing circuit, causes the processing circuit to:

cause a video decoder of a computing system to receive data of at least one of analog audio data and analog video data, wherein a line of the data includes screen end information, a data access parameter, color burst information, and at least one of audio and video data and wherein the data access parameter is independent of a source of the data;

digitizing, independent of the data access parameter, at least one of audio and video data to produce a digital signal, wherein once the at least one of audio and video data is digitized, the data access parameter is lost;

prior to enabling a central processing unit to access the digital signal, determine whether the data access parameter restricts accessing of the digital signal; and

when the data access parameter restricts accessing of the digital signal, prevent the central processing unit from accessing the digital signal without restriction.

5. (allowed) The video decoder of claim 14, wherein the memory further comprises programming instructions that, when read by the processing circuit, causes the processing circuit

to receive the data from at least one of: a digital video disc driver within the computing system, a video cassette recorder, and a video transmission source.

6. (allowed) The system of claim 4, wherein the accessing performed by the central processing unit further comprises copying the digital signal.

7. (allowed) The system of claim 4, wherein the accessing performed by the central processing unit further comprises providing the digital signal to a display device.

8. (allowed) The system of claim 4, wherein the digital signal further comprises audio and/or video data.

9. (allowed) The system of claim 4, wherein the data access parameter includes copy restriction information.

10. (allowed) A digital storage medium that stores programming instructions that, when read by a processing device, causes the processing device to detect protection of at least one of audio and video, the digital storage medium comprises:

first storage means for storing programming instructions that, when read by the processing device, causes the processing device to cause a video decoder of a computing system to receive data of at least one of analog audio data and analog video data, wherein a line of the data includes screen end information, a data access parameter, color burst information, and at

least one of audio and video data and wherein the data access parameter is independent of a source of the data;

second storage means for storing programming instructions that, when read by the processing device, causes the processing device to digitize, independent of the data access parameter, the at least one of audio and video data to produce digital video, wherein, once the at least one of audio and video data is digitized, the data access parameter is lost;

third storage means for storing programming instructions that, when read by the processing device, causes the processing device to contemporaneous with the digitizing and prior to enabling a central processing unit to access the digital video, determine whether the data access parameter restricts accessing of the digital video; and

fourth storage means for storing programming instructions that, when read by the processing device, causes the processing device to, when the data access parameter restricts accessing of the digital video, prevent the central processing unit from accessing the digital video without restriction.

11. (previously presented) A method for a computing system to provide protection of incoming data, the method comprising:

receiving data of at least one of analog audio data and analog video data, wherein a line of the data includes screen end information, a data access parameter, color burst information, and at least one of audio and video data and wherein the data access parameter is independent of a source of the data;

digitizing, independent of the data access parameter, at least one of audio and video data to produce digital video, wherein once the at least one of audio and video data is digitized, the data access parameter is lost;

prior to enabling a central processing unit to access the digital video, determine whether the data access parameter restricts accessing of the digital video; and

when the data access parameter restricts accessing of the digital video, prevent the central processing unit from accessing the digital video without restriction.

12. (previously presented) The method of claim 11 wherein the incoming data includes an embedded data access parameter and wherein the method includes storing the digital video in memory wherein the stored digital video in the memory does not include the embedded data access parameter.

13. (previously presented) The method of claim 11 wherein preventing the central processing unit from accessing the digital video without restriction includes controlling access to the digital video to provide at least one of: copy restriction, viewing restriction and use restriction of the digital video.

14. (previously presented) The method of claim 13 wherein providing at least one of: copy restriction, viewing restriction and use restriction of the digital video includes controlling access to the digital video to provide a viewing option, parental control, still frame copy restriction, copying with copyright notices, and reduced quality copying.

15. (previously presented) A computing system to provide protection of incoming data that includes an embedded data access parameter comprising:

a video digitizer circuit operative to receive data of at least one of analog audio data and analog video data, wherein a line of the data includes screen end information, a data access parameter, color burst information, and at least one of audio and video data and wherein the data access parameter is independent of a source of the data and digitize, independent of the data access parameter, at least one of audio and video data to produce digital video, wherein once the at least one of audio and video data is digitized, the data access parameter is lost;

memory operatively coupled to the video decoder, for storing the digital video wherein the stored video data does not include the data access parameter;

a protection detection circuit operative to detect the presence of the embedded data access parameter and provide an indication of protection based on the embedded data access parameter when the embedded data access parameter is detected wherein the indication of protection indicates one of a plurality of different types of data access; and

at least one of: a central processing unit and another computer element, responsive to the indication of protection from the protection detection circuit and operative to process the stored video data based on the indication of protection.

16. (previously presented) A method for a computer system to protect access to video data received from an analog video signal that includes an embedded data access parameter comprising:

receiving an indication of data access restriction for stored digital video data that is stored in memory, based on the embedded data access parameter, wherein the stored digital video data does not include the embedded data access parameter from the analog video signal; and

processing the stored digital video data in accordance with the received indication of data access restriction.

17. (previously presented) The method of claim 16 wherein the indication of data access restriction indicates one of a plurality of different types of data access of the stored digital video data and wherein processing the stored digital video data in accordance with the received indication of data access restriction includes controlling access to the stored digital video data to provide at least one of: copy restriction, viewing restriction and use restriction of the digital video data.

18. (previously presented) The method of claim 17 wherein controlling to provide at least one of: copy restriction, viewing restriction and use restriction of the digital video includes controlling access to the stored digital video data to provide at least one of a viewing option, parental control, still frame copy restriction, copying with copyright notices, and reduced quality copying.

19. (previously presented) A computer system to protect access to video data received from an analog video signal that includes an embedded data access parameter comprising:

memory containing stored digital video data obtained from the analog video signal wherein the stored digital video data does not include the embedded data access parameter from the analog video signal; and

at least one of: a central processing unit, a computer element and a peripheral device, operatively coupled to the memory, and operative to receive an indication of data access restriction for stored digital video data that is stored in memory, based on the embedded data access parameter, and operative to process the stored digital video data in accordance with the received indication of data access restriction.

20. (previously presented) The computer system of claim 19 wherein the indication of data access restriction indicates one of a plurality of different types of data access of the stored digital video data and wherein the at least one of the CPU, computer element and peripheral device processes the stored digital video data in accordance with the received indication of data access restriction and includes controlling access to the stored digital video data to provide at least one of: copy restriction, viewing restriction and use restriction of the digital video data.

21. (previously presented) The computer system of claim 20 wherein the at least one of the CPU, computer element and peripheral device provides at least one of: copy restriction, viewing restriction and use restriction of the digital video by controlling access to the digital video data to provide at least one of a viewing option, parental control, still frame copy restriction, copying with copyright notices, and reduced quality copying.

22. (new) A method comprising:

processing received data including content protection coding signifying a first level of content protection, in a data processing system;

independently of the content protection coding in said received data, imposing on said processing system a requirement for received data to be subject to a second level of content protection;

selecting one of the first and second levels of content protection; and

restricting access to the received data based on the selected level of content protection.